

Position Paper on the Revised Payment Services Directive & Regulation

Introduction

The European FinTech Association (EFA) welcomes the European Commission's (Commission) proposals for a new Payment Services Directive (PSD3) and Regulation (PSR). PSD2 has delivered a more innovative, competitive payments landscape in Europe, allowing consumers to benefit from new products and services and more secure payments. However, challenges remain, and while it is encouraging to see these addressed in the proposals, EFA would like to encourage the co-legislators to pay particular attention to the following areas: safeguarding, transparency in cross-border payments, open banking, access to payment systems, and consumer protection.

Key messages:

- The EFA is enthused about the levelling of the playfield between banks and non-banks by amending the scope of the Settlement Finality Directive (SFD). However, to avoid further delay, the SFD should be amended as quickly as possible via the ongoing negotiations on the Instant Payments Regulation (IPR).
- The EFA encourages the co-legislators to ensure that PIs ability to safeguard funds with the central bank becomes available, preventing the encouragement to shop around for central bank safeguarding accounts.
- We suggest several further adjustments to the SCA rules that could be made to foster innovation and customer convenience while maintaining high standards of security, including future proving of SCA, SCA in the corporate context, marketplaces/platforms, and outsourcing arrangements.
- The EFA brings forward several concerns and suggestions on improving open banking, including the prohibition of contracts model, re-authorisation, dedicated interfaces, account access and permissions, transparency and information about the execution of payments, and variable recurring payments.
- The EFA recommends further clarifying the definition of “agents” and harmonising it across Member States to reflect market realities.
- The EFA is concerned that the proposed transparency provisions for cross-border and one-leg-out payments will not lead to the envisioned results because consumers cannot effectively compare providers when sending money abroad. Thus, a benchmark rate should be introduced.
- The EFA is convinced that IBAN discrimination should be further addressed and enforced by imposing clear obligations, establishing a robust enforcement system, creating a user-friendly EU-wide platform for reporting IBAN discrimination, and establishing a pan-European forum for regulators and policymakers.
- The EFA welcomes the additional measures to protect consumers against fraud. These include measures on fraud investigation and prevention, APP fraud, returning funds to fraud victims, and the responsibility of online platforms and telcos.
- Regarding fraud-data sharing, the EFA calls for the co-legislators to clarify rules on such data-sharing and include a clause for standardisation of fraud-data sharing arrangements.
- The EFA calls for the PSR and PSD3 to clarify the clauses of PSD2, which have led to fragmented implementation across the Member States, and to ensure the two legislative pieces will respect the “same business, same rules” principle, lifting the prohibition for EMIs to grant pass on interest to their customers.

Direct access to payment systems for non-bank PSPs.

EFA welcomes the proposed changes enabling payment and e-money institutions (PIs/EMIs) to access payment systems designated under the Settlement Finality Directive (SFD). Despite this, EFA is convinced that these amendments to the SFD should be introduced via the Instant Payments Regulation (IPR) to avoid any delays in EMIs and PIs accessing the payment systems. Non-banks have been disadvantaged for too long - to reap the benefits of direct access, the deadline for transposing the SFD amendments in the Member States should be minimised to a maximum of 6 months.

It is reassuring that payment system operators will be required to set proportional and non-discriminatory risk criteria, reducing differences in access due to the regulatory license held by each institution. We encourage co-legislators to prevent de-risking, as PSOs may not explicitly discriminate based on license but may implicitly prevent PIs and EMIs from directly accessing payment systems by taking a very rigid approach to their access criteria. EFA highly supports a risk assessment before granting direct access to the relevant payments infrastructure. However, it is worth highlighting that regulators should have a deep knowledge and understanding of the firms they supervise to ensure they appropriately calibrate risks to the payment system - whether firms connect directly or indirectly. Certain risks to the payment system may exist even when a non-bank is indirectly connected. As an organisation with many non-bank Payment Service Provider (PSP) members, the EFA offers to work with the co-legislators throughout establishing the relevant safeguards around direct access.

Safeguarding.

The PSD3 proposal includes the possibility for PIs to safeguard funds with the central bank at the central banks' discretion. The EFA encourages the co-legislators to ensure that this option truly becomes available and avoid a scenario where shopping around for central bank safeguarding accounts is encouraged.

Safeguarding at the central bank would add choice for PIs as they diversify their safeguarding options, especially given the stronger requirements in the Commission's proposal to ensure firms have a diversified way of safeguarding funds. This would help reduce concentration risk, lower the risk profile of safeguarded funds, mitigate third-party de-banking risks, and increase consumer trust in safeguarded funds.

The EFA suggests that safeguarding letters be harmonised, using the same or similar templates across the Union. This template could also be used by central banks and would greatly reduce the administrative requirements for non-bank PSPs. In addition, banks and central banks should be required to set out a reasoned explanation in cases where they refuse a safeguarding account to PIs or EMIs to minimise safeguarding de-risking.

De-risking.

EFA welcomes the stronger language on de-risking in the Commission's proposal and believes the provisions will help avoid blanket de-risking of the non-bank sector. We encourage introducing a minimum timeline and propose giving at least 6 months' notice before off-boarding. This would also allow a non-bank to address the concerns banks may have raised in their reasoning and might avoid off-boarding altogether. This will contribute to making the non-bank payment sector more secure.

Strong customer authentication.

The EFA welcomes clarifications around the application of Strong Customer Authentication (SCA) rules to merchant-initiated transactions (MIT) and mail and telephone orders (MOTO). In general, PSD2 and the

accompanying RTS on SCA and CSC have left too much room for interpretation by different counterparties involved in a transaction, e.g., there is no agreed standard on the obligations TPPs have.

The EFA notes that further adjustments to the SCA rules could be made to foster innovation and customer convenience while maintaining high standards of security. As such, there should be a structured approach to the EBA consulting with industry to update SCA where necessary and to ensure the rules are still fit for purpose considering market, technological, and economic developments since the introduction of SCA. As part of this, the EFA stresses that the application of SCA in the corporate context, i.e., where the payer is acting in a corporate capacity and not as an individual consumer, should be revised. Given the challenges of implementation (e.g., a corporate employee using personal rather than company details to authenticate themselves) and significantly lower fraud risk associated with corporate authentication (e.g., where a corporate employee should not have to re-authenticate after 5 minutes of inactivity given the business context), the EBA should issue further guidance and clarifications that ensure proportionate application of SCA in the corporate context. In addition, additional exemptions for SCA should be considered for specific cases, such as using the same gateways to make recurring payments or for merchants' refunds. There should be more consideration given to SCA for marketplaces or platforms, which are a common structure in Europe - exemptions could be applied at the platform level (treating the platform as the payee) rather than requiring individual sellers on the platform to be identified as payees which significantly decreases the usefulness of most of the SCA exemptions, e.g. recurring payments. SMEs should also be subject to a more proportionate application of SCA requirements and could be allowed to use secure alternatives to SCA. Furthermore, clearer guidance is needed regarding Transaction Risk Analysis (TRA) and associated fraud ratio calculations. Additional thresholds could be introduced in TRA exemptions to increase the use of TRA. The threshold for low-value transaction exemptions could be increased, and the approval process regarding secure corporate payments with competent authorities should be accelerated.

Ideally, protecting merchants and consumers from fraud is best done through technology-neutral regulation focusing on outcomes rather than prescriptive rules. The EFA welcomes the use of behavioral biometrics and environmental factors in the provisions on transaction monitoring, and proposes considering their use as part of the range of inherence factors that can be used for SCA. In addition, the flexibility introduced for the use of categories in two-factor authentication (with the possibility to use two factors from the same category) should be maintained. The no-mobile-only approach could also be problematic, particularly in the context of increased use of such devices for everyday activities of EU citizens of all ages, including those with limited digital skills. Furthermore, it should not be the back-end ASPSP, but the customer-facing TPP who decides which of the available authentication methods should be used in a given context, e.g. at physical point-of-sale, where it is clear that the payer is using a mobile.

Additionally, the EFA emphasises that technical service providers that participate in the authentication should be obliged to provide all relevant details of the authentication to the PSP. In our view, the introduced outsourcing arrangements would be almost impossible to implement as it would require providers of such solutions to contract with a large number of PSPs and allow such PSPs to monitor them. Technical service providers do not often consider these solutions their main business model and are, therefore, unwilling to go through these processes with each PSP.

Open banking

The PSD2 framework for open banking has successfully stimulated data-driven solutions to real-world financial problems for EU citizens and businesses; EFA members are stoking competition and product innovation, an improved banking experience, and new ways for consumers to engage with and manage their finances. There is much more utility and value that open banking can drive, including in conjunction with parallel reforms to broaden the coverage of SEPA instant payments. Therefore, the EFA welcomes the renewed focus on open banking in the PSR and is convinced that several steps should be taken to achieve the full potential of open banking in the EU.

- Prohibition of contracts model

Under PSD2, Account Servicing PSPs (ASPSPs) must provide access to their customers' payment accounts to Payment Initiation Service Providers (PISPs) at no cost and without needing a contract between the bank and the PISP. This model has stimulated competition and market entry and has kept the cost base for open banking providers low. In turn, these providers can offer merchants cost-effective payment initiation services.

The EFA is convinced that removing this prohibition on contracts will jeopardise the adoption of open banking and create a system that replicates cards, hampering competition in the payments market. Therefore, we encourage the co-legislators to keep the non-compensatory model for baseline open banking services. Beyond the baseline open banking services outlined in the PSR, there is ample room for industry collaboration towards added-value, commercial services, both bilaterally and through multilateral forums like the SEPA Payment Account Access Scheme (SPAA).

- Re-authorisation

The EFA supports a streamlined process for PIs and EMIs to re-authorise under the PSD3 that does not create unnecessary administrative bottlenecks. There should be a clear path to simple re-authorisation under PSD3 for existing PIs and EMIs demonstrating compliance to their National Competent Authority (NCA) and a presumption of automatic re-authorisation of firms that already have a very high level of regulatory oversight by their competent authorities subject to firms' compliance with additional PSD3 requirements. EMIs and PIs should only have to satisfy new PSD3 authorisation requirements and not re-submit information shared previously with their competent authority. This limits duplication in licensing processes and ensures a level playing field for all e-money institutions. Furthermore, it should be clarified that AIS and PIS activities can be provided by the same legal entity despite having different rules, e.g., regarding storing sensitive data.

- Dedicated interfaces

The EFA welcomes and supports the Commission's proposal for additional performance and functionality requirements for Application Programming Interfaces (APIs) and provisions on enhancing supervision and enforcement practices and notes that they could be strengthened even further by involving the European and National Competition Authorities in a decisive manner.

EFA is convinced that, if an API is dedicated to TPPs, then there must be a contingency, not only for the case of non-availability but also for other non-performance, e.g., lack of any required functionality. Given that FIDA shall not cover any transaction initiations, we believe that PSR should extend the scope of 'payment accounts' to saving accounts, as is already the practice in some Member States.

We also welcome the focus on removing API and SCA barriers by including a list of prohibited obstacles to open banking based on previous work carried out by the EBA. However, to future-proof the PSR, the list needs to be non-exhaustive to cover current and future obstacles.

- Account access and permissions

The EFA emphasises that whilst mandating an AISP and its initial access should require an SCA, any subsequent access is secured by the Account Information Service Provider's (AISP) eIDAS certificate and should not require any customer action, let alone further SCAs, especially considering that the proposal enables customers to withdraw any consent easily via the "permissions dashboard" which shall be offered by the ASPSP. However, it should be clarified that the information displayed on the dashboard must be provided exclusively by the TPP, who was given the permissions, not by the ASPSP, who was not involved and would not have such information.

Separately, merchant-facing PISPs contract with merchants and act solely on their behalf. Therefore, they should not need any contract with the payer, not even a single payment contract. Any form of GDPR-legal ground for processing the payer's data (e.g. consent) should be sufficient.

- Information about the execution of payments

The EFA highlights that ASPSPs should be required to immediately confirm whether any initiated payment will be executed or not so that PISPs can inform merchants in real-time and thereby compete on a level playing field with other payment solutions, e.g. cards. For this, it is important to ensure that at least information exchange for confirmation of the transaction execution and the reasons for transaction failure are standardised, and enforcement measures are efficient. If an ASPSP is not able to do that, PISPs should be allowed to access account information, e.g., the available balance and past transactions, prior to initiating a payment, so that it can be stopped if the non-execution risk is deemed too high.

- Variable recurring payments

The EFA is convinced that PSD3 should make variable recurring payments clearly defined and mandated for sweeping (automated money transfer between customers' own accounts, e.g., to move any excess balance at the end of the month from a checking to a savings account). This would be a huge step forward in delivering competition and innovation to consumers and has already been successfully implemented in the UK. In the UK, the implementation of sweeping variable recurring payments showed its effectiveness by allowing customers to make smarter savings by automatically moving surplus funds out of current accounts into savings accounts, avoiding overdrafts, and creating competition among ASPSPs.

Furthermore, the EFA suggests having more proportional requirements for AISPs and PISPs where no fund handling is involved, therefore avoiding the imposition of cumbersome AML requirements. In addition, the EFA notes that under PSD2, the regulatory treatment of online marketplaces and payment facilitators (Payfacs) – increasingly important parts of the EU's digital economy – is unclear and interpreted differently across the Member States. For PSPs to better serve this market, a clearer and more consistent approach to regulating marketplaces and Payfacs should be developed.

Definitions.

The EFA suggests further clarifying the definition of "agents," which should be harmonised across Member States in order to reflect evolving market realities. It should be reiterated that marketplaces and platforms supported by

PSPs, which remove them from control or possession of funds for third parties, are not, by default, agents of the PSP. In addition, there is an increasing prevalence of multi-processor set-ups for payment acquiring services, where, in particular, large businesses rely on the services of several acquirers. When acquirers use agents to deliver their services, it should be noted that every agent only acts on behalf of one acquirer as their principal (PSP) and not in respect of all payment services provided to the payment services user.

Transparency provisions for cross-border and one-leg-out payments.

It is encouraging to see that the PSR acknowledges that too much money is lost to hidden FX fees in remittances and cross-border payments more generally. The EFA agrees that including one-leg-out payments into the scope of the PSR will ensure that the EU has better tools available to tackle their high cost. However, we observe that today, people and businesses are unable to effectively compare providers when sending money abroad. While we are very encouraged by the fact that charges for currency conversion and foreign exchange rate mark-ups are now explicitly recognised as charges that must be clearly disclosed, we are concerned that the proposed disclosure will not address the problem. Therefore, the EFA calls for the co-legislators to introduce a benchmark rate - an aggregated mid-market rate provided by neutral, independent actors - to ensure consumers can accurately compare the cost across providers. Relying on a stale European Central Bank (ECB) rate will not account for intraday movements.

IBAN discrimination.

Many of EFA's members' customers still face IBAN discrimination daily. As open banking was increasingly taken up by the EU citizens, discrimination also happens via these newer payment methods. While the EFA is glad to observe the inclusion of the ban on discrimination based on domestic identifiers in the open banking context within the PSR, we are convinced that the co-legislators should go further to prevent the lack of enforcement on which IBAN discrimination has thrived. To fight IBAN discrimination, EFA proposes several key actions that could be included within the PSR:

- Imposing clear obligations on PSPs, merchants, and public entities to accept non-local IBANs, whilst:
- Establishing a robust enforcement system, granting NCAs the authority to impose fines and sanctions on those failing to comply with anti-IBAN discrimination rules.
- Creating a user-friendly EU-wide platform for reporting IBAN discrimination to address the underreporting of IBAN discrimination cases and some NCAs only investigating cases reported through official channels. This centralised reporting system could ensure prompt forwarding of cases to the relevant NCAs and allow tracking of IBAN discrimination instances at the EU and national levels.
- Establishing a pan-European forum for regulators and policymakers to exchange information and share best practices to make progress in combating IBAN discrimination.

Additionally, EFA members see a certain level of discrimination on the level of the national alternative payment methods. For certain schemes, to become a direct participant, PSP needs to be connected to the national infrastructure of the particular Member State. We believe such practices restrict competition, hinder the development of a truly Digital Single Market and directly contradict EU legislation.

Consumer protection.

- Fraud investigation

The current refund timeline for unauthorised transactions is immediately or no later than the next business day and is only extended to 10 days for highly suspicious cases. EFA is concerned that this creates an easy way for false

claimers to obtain refunds as the PSP does not have appropriate time to make an informed decision or conduct a proper investigation. To make a reasoned judgment as to whether there could be fraudulent behaviour or gross negligence by the customer, the PSP should be given the opportunity to appropriately review the case. The strict timelines can incentivise the PSP to automatically approve or decline a part of the oncoming claims just to meet the deadline. This, in turn, can create a vulnerability that false claimers can abuse and reduce the quality of responses received by legitimate customers.

Additionally, the PSR should clearly indicate that the PSP should be able to further investigate the claim or refuse the refund to the customer in cases of gross negligence by the customer. But to do so, the concepts of 'gross negligence' and 'high suspicion of fraudulent behaviour' should be further expanded. It would be beneficial to further clarify the parameters for establishing a gross negligence case or when a PSP can deem there is a high suspicion of fraudulent behaviour or introduce a concept of customer standard of caution.

- APP fraud

With Authorised push payment (APP) fraud becoming one of the most challenging and complex issues, the EFA understands the need for rules around reimbursement for impersonation fraud. However, the mitigating measures for APP fraud are frequently outside the control of the PSP, and there is no direct causal link between the actions of a PSP and a customer falling victim to APP fraud. At the same time, the PSR creates a new liability regime for APP fraud without proven responsibility on the PSP side and the establishment of a causal link. We also see several unintended outcomes for such a regime, such as risk to competition and the sustainability of FinTechs whose focus is on instant payments. Therefore, EFA believes that PSPs should be liable for impersonation scams only if the PSP had control over the specific impersonation scam that took place.

In case co-legislators agree with the proposed option for strengthening protection against fraud, we suggest clarifying the rules to minimise the costs for PSPs and encourage users to take greater precautions before authorising a payment. On average, users make several transactions before a fraudster receives the full desirable amount. Therefore, we believe that it is important to introduce an upper and lower threshold for reimbursement to ensure that customers work with their PSPs to conduct due diligence and take time to consider any transfer considered risky. If customers were aware of this, they would take much greater precautions before authorising a payment. To avoid different application of rules across Member States, we also call for more clarity on what is considered to be bank employee impersonation fraud. For instance, current provisions give rise to the question of whether it is enough for a fraudster to use the name of a company in communication or if the email address and telephone number need to be exploited. Additionally, we believe it is important to provide an obligation on the users' side to cooperate with a PSP, and provide sufficient and truthful evidence.

- Telcos' role in fighting fraud

EFA welcomes that telcos should play a part in addressing fraud but does not believe the current provisions go far enough. There is no liability for electronic communication or online platform services, and the full liability for refunding the customer rests with the PSP. This is problematic as data from other jurisdictions shows that 70% of authorised push payment scams started on an online platform, defined as emails, social media, websites (including auction sites), and apps (including dating apps). Looking into specific scam categories, most investment (96%), romance (96%), and nearly all purchase (98 %) scams originated online. Often, these are paid-for advertisements, meaning that social media companies are profiting from fraudulent ads while the finance

sector bears the brunt of the cost. The co-legislators should ensure that consumers are adequately protected and ensure online platforms, as well as telcos, share in the responsibility.

- Rules on blocking and retrieving stolen funds

Additionally, to protect customers from the loss of funds, we believe it's important to ensure that there are clear rules on blocking and retrieving stolen money to return it to fraud victims. Currently, EFA members encounter issues when, after identifying a case of fraud and blocking the funds that the customer acquired from illegal activities, there is no legal option to return these funds to the victim. Some jurisdictions have developed market practices (e.g., France, Ireland, Belgium, Netherlands, Italy, and Germany) where funds can be repatriated after the information has been provided by the payer's PSP. However, such practices do not have a pan-European reach. In some Member States, the lack of clarity around repatriation not only prevents PSPs from returning back stolen money to the victims of scam but also creates obstacles to cross-border cooperation.

- Alignment with the Instant Payments Regulation

Finally, the provisions on extending payee verification to SEPA credit transfers should ensure alignment between the Instant Payments Regulation and the PSR, and that information used for verification can include unique identifiers in addition to IBANs. This ensures that an EU verification scheme can account for different types of account identifiers, including where a unique IBAN is not assigned.

Fraud data sharing.

PSR takes a huge step towards enhancing fraud prevention mechanisms by allowing PSPs to voluntarily enter the information-sharing arrangements to better detect fraudulent payment transactions and protect their customers. According to the Explanatory Memorandum to the PSR, such information should include personal data such as unique identifiers of a payee. The EFA emphasizes the importance of clarifying such intent in the text, as sharing the names of account holders involved in fraudulent activities would increase the capacity of PSPs to prevent unlawful transactions. We are also concerned that these provisions will have a declarative character unless industry-wide standards for fraud data-sharing arrangements are established. Without a certain level of standardisation, PSPs would need to enter multiple information-sharing arrangements and adapt their systems to each one, as PSPs operate differently.

Additionally, data sharing just among PSPs would limit the effectiveness of such arrangements. The ecosystem should at least include public entities, telcos, and online platforms to stop potential fraud before it happens and minimise the number of payments stopped unnecessarily.

Legal certainty.

PSD2 has been interpreted and implemented inconsistently by individual Member States, which is skewing competition and working against creating a single market for payment services. This can, for example, be seen in the different interpretations of the definition of "agent". In certain Member States, the definition of agent has been interpreted as including promotional activities, and have consequently asked for a central contact point to be set up. PSD3 can avoid such shortcomings by clarifying those definitions that have proved to be a source of regulatory fragmentation.

We welcome the transition of the key regulatory framework in PSD2 into a Regulation through the introduction of the new Payment Services Regulation. This will ensure a more consistent application across EU Member States and strengthen the regulation's role in driving payment innovation.

Same business, same rules principle

Despite the Payments Package's general aim to harmonise the regime for all PIs, it still upholds the prohibition for EMI's to pass on interest to their customers. This puts them at an unjustified competitive disadvantage compared to other PIs while not respecting the "same business, same rules" principle.

About us:

*The European FinTech Association (EFA) is a not-for-profit organization representing leading FinTech companies of all sizes from across the EU. It brings together a diverse group of 40+ FinTech providers ranging from payments, to lending, banking, robo-advice, investment as well as software-as-a-service for the finance sector, with a clear focus on enabling a single market for digital financial services. For more information, visit www.eufintechs.com or follow **@EFAssociation** on Twitter.*